

ETSI TS 119 442 V1.1.1 (2019-02)



Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services

Signatures and Infrastructure Services for trust service providers Digital signature validation standards

ReferenceDTS/ESI-0019442

Keywords

electronic signature, protocol, validation**ETSI**

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.
All rights reserved.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.

oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and
of the oneM2M Partners.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	7
Foreword.....	7
Modal verbs terminology.....	7
1 Scope	8
2 References	8
2.1 Normative references	8
2.2 Informative references.....	9
3 Definition of terms, symbols, abbreviations and terminology	10
3.1 Terms.....	10
3.2 Symbols	12
3.3 Abbreviations	12
3.4 Terminology	12
4 Technical approach to the specification of the protocols	12
4.1 Main features	12
4.2 General requirements	14
4.3 XML protocol.....	15
4.3.1 Introduction.....	15
4.3.2 Redefined DSS-X types	15
4.4 JSON protocol.....	16
4.4.1 Introduction.....	16
4.4.2 Extension of DSS-X types	16
5 Protocol for validation of AdES signatures.....	17
5.1 Request message	17
5.1.1 Component for requesting validation	17
5.1.1.1 Component semantics.....	17
5.1.1.2 XML component	17
5.1.1.3 JSON component	18
5.1.2 Component for submitting signature to be validated	18
5.1.2.1 Component semantics	18
5.1.2.2 XML components	19
5.1.2.3 JSON component	20
5.1.3 Components for submitting signed documents or representations of the signed documents	20
5.1.3.1 Components semantics.....	20
5.1.3.2 XML components	21
5.1.3.2.1 General requirements.....	21
5.1.3.2.2 Additional requirements for contents of dss2 : InputDocuments	21
5.1.3.3 JSON components.....	22
5.1.3.3.1 General requirements.....	22
5.1.3.3.2 Additional requirements for contents of inDocs	23
5.1.3.4 Cardinalities for elements used for sending signatures, signed documents and representations of signed documents	24
5.1.4 Optional components	24
5.1.4.1 Container for optional components	24
5.1.4.1.1 Component semantics.....	24
5.1.4.1.2 XML component	25
5.1.4.1.3 JSON component.....	26
5.1.4.2 New components defined in the present document	27
5.1.4.2.1 Component for identifying the signatures to be processed (signatures-to-process-refs container).....	27
5.1.4.2.2 Component for requesting validation against a certain signature policy	30
5.1.4.2.3 Component for requesting a detailed validation report (signed or unsigned)	31
5.1.4.2.4 Component for passing proofs of existence of one or more signatures	32
5.1.4.3 Components re-used from DSS-X core v2.0.....	34
5.1.4.3.1 Component for identifying under which service policy the validation has to be conducted	34

5.1.4.3.2	Component for requesting notifications in a certain language	34
5.1.4.3.3	Component for allowing the client to claim its identity	34
5.1.4.3.4	Component for passing schemas	35
5.1.4.3.5	Component for requesting to set the validation time to a certain value.....	35
5.1.4.3.6	Component for requesting to return the validation time.....	36
5.1.4.3.7	Component for passing validation material to the server	36
5.1.4.3.8	Component for requesting return of the signing time.....	36
5.1.4.3.9	Component for requesting the server to return the identity of the signer	36
5.1.4.3.10	Component for requesting the server to return the result of transforming the input document	37
5.1.4.3.11	Component for requesting to return the validation of signed ds:Manifest in XAdES signatures	37
5.2	Response message	38
5.2.1	Component for responding to a validation request	38
5.2.1.1	Component semantics	38
5.2.1.2	XML component	38
5.2.1.3	JSON component	38
5.2.2	Component for the global validation result.....	39
5.2.2.1	Component semantics	39
5.2.2.2	XML component	39
5.2.2.3	JSON component	39
5.2.3	Optional components	39
5.2.3.1	Container for optional components	39
5.2.3.1.1	Component semantics.....	39
5.2.3.1.2	XML component	40
5.2.3.1.3	JSON component.....	40
5.2.3.2	New components defined in the present document.....	41
5.2.3.2.1	Signature processing results container.....	41
5.2.3.2.2	Component for referencing the validated signature.....	43
5.2.3.2.3	Component for notifying the signature policy applied during the validation	43
5.2.3.2.4	Component for notifying the signature policies under which the server can conduct validation	44
5.2.3.2.5	Component for returning the detailed validation report (signed or unsigned).....	45
5.2.3.3	Components re-used from DSS-X core v2.0	46
5.2.3.3.1	Component for indicating the applied service policy	46
5.2.3.3.2	Component for indicating validation time.....	47
5.2.3.3.3	Component for returning the signing time of one signature	47
5.2.3.3.4	Component for returning signer's identity	47
5.2.3.3.5	Component for returning the result of transforming the input document	48
5.2.3.3.6	Component for returning the result of validating ds:Manifest elements in XAdES signatures	48
6	Protocol for augmentation of AdES signatures	49
6.1	Request message	49
6.1.1	Component for requesting augmentation of signatures.....	49
6.1.1.1	Component semantics	49
6.1.1.2	XML component	49
6.1.1.3	JSON component	50
6.1.2	Additional inputs	51
6.1.2.1	Container for additional inputs	51
6.1.2.1.1	Semantics.....	51
6.1.2.1.2	XML component	51
6.1.2.1.3	JSON component.....	52
6.1.2.2	Component for identifying the level the signatures are requested to be augmented to	52
6.1.2.2.1	Component semantics.....	52
6.1.2.2.2	XML component	54
6.1.2.2.3	JSON component.....	54
6.1.2.3	Component for identifying the quality level of the time-stamp tokens used in the augmentation process.....	54
6.1.2.3.1	Component semantics.....	54
6.1.2.3.2	XML component	54
6.1.2.3.3	JSON component.....	54
6.2	Response message	55
6.2.1	Component for responding to augmentation request	55
6.2.1.1	Component semantics	55
6.2.1.2	XML component	55

6.2.1.3	JSON component	56
6.2.2	Component for the global augmentation result.....	57
6.2.2.1	Component semantics	57
6.2.2.2	XML component	57
6.2.2.3	JSON component	57
6.2.3	Augment signature result container	57
6.2.3.1	Component semantics	57
6.2.3.2	XML component	57
6.2.3.3	JSON component	58
7	Protocol for validation and augmentation of AdES signatures	59
7.1	Request message	59
7.1.1	Component for requesting validation and augmentation	59
7.1.1.1	Component semantics	59
7.1.1.2	XML component	59
7.1.1.3	JSON component	59
7.1.2	Components for submitting signatures and signed documents	59
7.1.3	Optional components	60
7.1.3.1	Container for optional components	60
7.1.3.1.1	Component semantics.....	60
7.1.3.1.2	XML component	60
7.1.3.1.3	JSON component.....	60
7.2	Response message	60
7.2.1	Component for responding to validation and augmentation request.....	60
7.2.1.1	Component semantics	60
7.2.1.2	XML component	61
7.2.1.3	JSON component	61
7.2.2	Component for the global validation and augmentation result	61
7.2.2.1	Component semantics	61
7.2.2.2	XML component	61
7.2.2.3	JSON component	61
7.2.3	Optional components	61
7.2.3.1	Container for optional components	61
7.2.3.1.1	Component semantics.....	61
7.2.3.1.2	XML component	61
7.2.3.1.3	JSON component.....	62
7.2.3.2	Signature processing results container	62
7.2.3.2.1	Component semantics.....	62
7.2.3.2.2	XML component	62
7.2.3.2.3	JSON component.....	62
7.2.4	Reporting results	62
7.2.4.1	Introduction.....	62
7.2.4.2	Reporting results in XML protocol	62
7.2.4.3	Reporting results in JSON protocol	62
8	Processing models	63
8.1	Introduction	63
8.2	Retrieving signature(s)	63
8.2.1	Retrieving XAdES signature(s)	63
8.2.2	Retrieving CAdES signature(s).....	64
8.2.3	Retrieving PAdES signature(s).....	64
8.2.4	Non retrieved signatures	65
8.3	Processing signature(s)	65
8.3.1	Validating signature(s).....	65
8.3.1.1	Validating XAdES signature(s).....	65
8.3.1.2	Validating CAdES signature(s).....	65
8.3.1.3	Validating PAdES signature(s)	65
8.3.2	Augmenting signature(s).....	65
8.4	Building response message	65
8.4.1	Introduction.....	65
8.4.2	Building the global result component	66
8.4.3	Building new optional outputs	67

8.4.3.1	Building the signature processing results container	67
8.4.3.2	Building component for referencing the processed signature	67
8.4.3.3	Building component for returning the (signed or unsigned) validation report.....	68
8.4.3.4	Building component for notifying the signature validation policy applied during the validation.....	68
8.4.3.5	Building component for returning the signature policies available.....	68
8.4.3.6	Building the augment signature result container	68
8.4.4	Building DSS-X re-used optional outputs	69
8.4.5	Building the response message	70
9	Asynchronous processing.....	71
9.1	Asynchronous operation for the three protocols.....	71
9.2	Components for sending a pending-request	72
9.2.1	Components semantics	72
9.2.2	XML component.....	72
9.2.3	JSON component	72
9.3	Component for identifying the initial request.....	72
9.3.1	Component semantics	72
9.3.2	XML component.....	72
9.3.3	JSON component	72
9.4	Component for identifying the initial response-pending message.....	72
9.4.1	Component semantics	72
9.4.2	XML components	73
9.4.3	JSON component	73
Annex A (normative):	XML and JSON Schema files	74
A.1	XML Schema file location for namespace http://uri.etsi.org/19442/v1.1.1#	74
A.2	JSON Schema file location for "\$schema" " http://etsi.org/19442/v1.1.1/json# "	74
Annex B (informative):	Bibliography.....	75
History	76	

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"must" and "must not" are NOT allowed in ETSI deliverables except when used in direct citation.

*Full standard:
https://standards.etsi.org/catalog/standards/sist/0fa8bcb-b0b1/
4eb8b9fc-c41cc4ca/etsi-ts-119-442-v1.1.1/2019-02
STANDARD REVIEW*

1 Scope

The present document specifies the semantics of a protocol for requesting to a remote server (and for receiving the corresponding response) the validation of AdES digital signatures compliant with the following ETSI deliverables: ETSI EN 319 122 [2], ETSI EN 319 132 [3], ETSI EN 319 142 [4], ETSI TS 101 733 [5], ETSI TS 102 778 [9], ETSI TS 101 903 [7], ETSI TS 103 171 [8], ETSI TS 103 172 [10] and ETSI TS 103 173 [6].

The present document specifies the semantics of a second protocol for requesting the augmentation of AdES digital signatures compliant with the aforementioned ETSI deliverables.

The present document also specifies the semantics of a third protocol for requesting the validation and augmentation of AdES digital signatures compliant with the aforementioned ETSI deliverables.

Finally, the present document specifies two bindings, each one in a different syntax (XML and JSON), for each of the aforementioned protocols.

As far as it has been possible and suitable, the protocols have re-used constructs of DSS-X core v2.0: "Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0" [1] (also identified as DSS-X core v2.0 hereinafter). The protocols define new features which are not supported by DSS-X core v2.0.

NOTE 1: The protocols specified in the present document do not include components for submitting to the server ASiC containers compliant with ETSI EN 319 162-1 [i.1], ETSI EN 319 162-2 [i.2], ETSI TS 102 918 [i.3], and ETSI TS 103 174 [i.4]. They do not include either components for reporting on the validation of signatures included within an ASiC container. However, clients can always extract individual signatures and groups of signed documents from ASiC containers and prepare and submit suitable requests to the server for these individual signatures and groups of signed documents.

NOTE 2: The protocols specified in the present document do not include components for submitting to the server time-stamp tokens for their verification. They do not include either components for reporting on the verification of time-stamp tokens. Protocols specified by OASIS DSS-X Technical Committees include this type of components.

NOTE 3: The present document builds on a draft OASIS Committee Specification as the final OASIS specification was not available at the time of publication of the present document. The present deliverable will then be updated when the OASIS Committee Specification is formally adopted.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] OASIS Committee Specification Draft 01: "Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0".

NOTE: Available at <http://docs.oasis-open.org/dss-x/dss-core/v2.0/csprd01/dss-core-v2.0-csprd01.pdf>.

[2] ETSI EN 319 122 (all parts): "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures".

- [3] ETSI EN 319 132 (all parts): "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures".
- [4] ETSI EN 319 142 (all parts): "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures".
- [5] ETSI TS 101 733 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".
- [6] ETSI TS 103 173 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".
- [7] ETSI TS 101 903 (V1.4.2): "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".
- [8] ETSI TS 103 171 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".
- [9] ETSI TS 102 778 (all parts): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles".
- [10] ETSI TS 103 172 (V2.2.2): "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".
- [11] ETSI TS 119 102-2 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report".
- [12] IETF RFC 5646: "Tags for Identifying Languages".
- [13] ETSI TS 119 102-1 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".
- [14] IETF RFC 3061 (February 2001): "A URN Namespace of Object Identifiers".
- [15] H. Andrews. JSON Schema draft 07: "JSON Schema Validation: A Vocabulary for Structural Validation of JSON", March 19, 2018.

NOTE: Available at <https://json-schema.org/draft-07/json-schema-validation.html>.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".
- [i.2] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".
- [i.3] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".
- [i.4] ETSI TS 103 174: "Electronic Signatures and Infrastructures (ESI); ASiC baseline profile".
- [i.5] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".

- [i.6] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".
- [i.7] W3C Recommendation (11 April 2013): "XML Signature Syntax and Processing. Version 1.1".
- [i.8] ISO 32000-1: "Document management -- Portable document format -- Part 1: PDF 1.7".

3 Definition of terms, symbols, abbreviations and terminology

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.6], ETSI TS 119 441 [i.5] and the following apply:

attachment reference container: sub-component of input documents container for transferring a reference to an underlying protocol attachment where either the signed document or the transformed document is placed

augment signature result container: response protocol component for transferring to the client the results of the process carried out by the server when trying to augment one signature

NOTE: This component is specified in clause 6.2.3 of the present document.

augmented signature container: response protocol container for transferring to the client an augmented non-embedded AdES signature

NOTE: The document with signature container and augmented signature container are components of response messages for the augmentation protocol and for the validation and augmentation protocol.

document container: sub-component of input documents container for transferring to the server one signed document or a reference to one underlying transport protocol attachment where the signed document is placed

document digest container: sub-component of input documents container for transferring to the server the digest of one signed document

document with signature container: response protocol container for transferring to the client one signed document embedding its signature(s) or a reference to one underlying transport protocol attachment where the signed document embedding its signature(s) is placed

embedded AdES signature: AdES signature placed within a document that it signs totally or partially

NOTE 1: A XAdES enveloped signature (a XAdES signature that signs a data object that contains the XAdES signature itself) is an example, but there may be other situations where a non enveloped XAdES signature is an embedded XAdES signature, for example a XAdES signature that is a component of a XML file, signs only one specific part of that XML file, and this signed part does not envelope the signature.

NOTE 2: The rationale for this definition is that the placement of the signature to be validated and the signed documents within the protocol messages depends on whether the signature is embedded or not, as specified in clause 5.1.2.

enveloped AdES signature: AdES signature placed within the portion of the document that it signs

NOTE: The portion signed by the signature can be either the whole document or a part of it. What makes the signature be enveloped is that the signature is placed within the signed portion of the document. If the signature is placed within the document but not within the signed portion, then the signature is embedded but not enveloped.

global result component: response protocol component for notifying to the client a generic result of the processing performed by the server following the request submitted by the client

NOTE: If the response contains one or more processing signature results containers this component instructs the client to check the signature processing results. Otherwise, the result has only processed one signature and this component provides the result of this processing.

input documents container: request protocol component for transferring to the server either the signed documents themselves, or the transformed documents, or the digest of the signed documents, or references to underlying transport protocol attachments where the signed documents or the transformed documents are placed

NOTE: For more information about transformations of signed documents, see W3C Recommendation (11 April 2013) [i.7].

representation of a (signed) document: either the (signed) document itself, its digest, or the result of applying to the (signed) document a certain set of known transformations

signature object container: request protocol component for transferring to the server either one non-embedded signature, or a reference to an embedded signature

EXAMPLE: For instance, the client can place a reference to the signature instead of the signature itself in this component when the signature is embedded within the signed document. In these situations, the client can include the signed document (and its embedded signature) within the input documents container and include a reference to the signature within the signature object container.

NOTE 1: From the definitions above, input documents container can contain signatures as long as they are embedded within documents. And signature object container can contain signed documents as long as they are fully enveloped by the signature. The basic principle for placement of signed documents and signatures is the following: a signature that in essence is a non-embedded signature (even if it envelopes a signed document) is placed in the signature object container; and an object that in essence is a document (even if it embeds a signature) is placed in or is referenced from the input documents object container.

NOTE 2: Input documents container and signature object container components are implemented by specific XML and JSON types and elements in the bindings defined by the present document.

signature processing results container: response protocol component including the optional outputs generated by the server when processing (validating, augmenting, or validating and augmenting) one specific signature

NOTE: This component is specified in clause 5.2.3.2.1 of the present document. The requests of the three protocols specified in the present document can contain more than one signature. This container includes all the optional outputs generated by the server when it processes one of these signatures. The response message can, consequently, contain one or more signature results containers.

signature reference component: request and response protocol component referencing one signature

NOTE: The XML binding of this component is specified in [11], which is copied in clause 5.1.4.2.4.2 of the present document. Clause 5.1.4.2.4.3 of the present document specifies a JSON binding for this component.

signatures-to-process-refs container: request protocol component that includes references to those signatures whose processing the client requests to the server

NOTE 1: See clause 3.4 of the present document on terminology for an explanation of the meaning of the term "processing".

NOTE 2: A request message can include more than one signature. This component allows the client to instruct the server to process (validate, augment, or validate and augment) a selected subset of them.

transformed document container: sub-component of input documents container for transferring to the server the transformed document or a reference to one underlying transport protocol attachment where the transformed document is placed

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CMS	Cryptographic Message Syntax
DSS-X	Digital Signature Services eXtended
DSSX, DSS-X	Digital Signature Services eXtended
ERS	Evidence Record Syntax
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OID	Object Identifier
RFC	Request For Comments
URI	Uniform Resource Identifier
URN	Uniform Resource Name
UTC	Universal Time Coordinated
XML	eXtensible Markup Language

3.4 Terminology

The term "digest of the document", "document" being one of the documents signed by one signature submitted to a server within the request of any of the three protocols defined in the present document, is understood as indicated below:

- If the document is signed by a CAdES signature, it is the digest of the signed document itself.
- If the document is signed by a XAdES signature, it is the digest computed as specified in W3C Recommendation (11 April 2013) [i.7].
- If the document is a PDF document signed by a PAdES signature built on CMS or CAdES, it is the digest computed as specified in ISO 32000-1 [i.8].

The term "process" applied to AdES signature means either "validate", or "augment", or "validate and augment" depending of the protocol where the term is used. If the term is used out of the context of one protocol it does mean the action performed by the server on the signature, which is one of the three actions aforementioned.

4 Technical approach to the specification of the protocols

4.1 Main features

The main features supported by the 'validation' protocol specified in the present document, which are not supported by DSS-X core v2.0 [1] are:

- 1) Supports requesting the validation of one or more PAdES signatures embedded in one PDF document, if the client submits it to the server. It supports the validation of one PAdES signature if the client only submits the digest of the document where the aforementioned signature is placed.
- 2) Supports, when the request message contains more than one signature, requesting the validation of a subset of them.

- 3) Supports requesting to the server the application of a certain signature validation policy for validating the AdES signature(s). The server may notify in the response, the signature validation policy applied. The server may notify the list of signature validation policies that it supports.
- 4) Supports requesting a signed or unsigned detailed validation report for each validated signature. The server may include one signed or unsigned validation report for each signature within the response. The server may also include one signed or unsigned validation report for several validated signatures.

NOTE: The ETSI TS 119 102-2 [11] defines a validation report that can contain details of the validation of one or more AdES signatures.

- 5) The server may generate one or more signature processing results containers, each one providing all the details (including the aforementioned signed or unsigned validation report) concerning the validation of one signature.

The main features supported by the 'validation and augmentation' protocol specified in the present document, which are not supported by DSS-X core v2.0 [1] are:

- 1) Supports requesting the validation and augmentation of one or more PAdES signatures embedded in one PDF document, if the client submits it to the server. It supports the validation and augmentation of one PAdES signature if the client only submits the digest of the document where the aforementioned signature is placed.
- 2) Supports, when the request message contains more than one signature, requesting the validation and augmentation of a subset of them.
- 3) Supports requesting to the server the application of a certain signature validation policy for validating the AdES signature(s). The server may notify in the response, the signature validation policy applied. The server may notify the list of signature validation policies that it supports.
- 4) Supports requesting a signed or unsigned detailed validation report for each validated signature. The server may include one signed or unsigned validation report for each signature within the response. The server may also include one signed or unsigned validation report for several validated signatures.
- 5) The server may generate one or more signature processing results containers, each one providing all the details (including the aforementioned signed or unsigned validation report) concerning the validation and the augmentation of one signature.

The main features supported by the 'augmentation' protocol specified in the present document are:

- 1) Supports requesting the augmentation of one or more XAdES signatures and of one or more of CAdES signatures. The incorporation of the signatures and the signed documents are as specified in DSS-X core v2.0 [1].
- 2) Supports requesting the augmentation of one or more PAdES signatures embedded in one PDF document, if the client submits it to the server. It supports the augmentation of one PAdES signature if the client only submits the digest of the document.
- 3) Supports, when the request message contains more than one signature, requesting the augmentation of a subset of them.
- 4) Supports submission of validation material required for augmenting the signatures.
- 5) Supports submission of the claimed identity of the client.
- 6) The server may generate one or more signature processing results containers, each one providing all the details concerning the augmentation of one signature.